REMARKS

This case has been carefully reviewed in light of the non-final Office Action dated December 20, 2007, wherein claims 1-38 were rejected as being obvious under 35 U.S.C. 103(a). Claims 1-38 were rejected as being obvious over Meltzer ("Vulnerability Detection Systems (VDS) FAQ", pages 1-13) in view of Bunker (US Patent Application No. 2003/0056116), while claims 1, 3, 15-16 and 29-30 were rejected as being obvious over Gleichauf (US Patent 6,324,656) in view of Barnett "NOOSE-Networked Object-Oriented Security Examiner", USENIX 2000, pages 369-378.

Claims 1-4, 29 and 30 have been amended to recite the invention even more clearly.

Claims 1-38 are pending. Reconsideration of the rejections in light of the following remarks is respectfully requested.

Swearing back Meltzer under 37 CFR 1.131

Meltzer, which was allegedly published on January 30, 2003 has been applied as a reference under 35 USC 102(a).

It is noted that the present Application claims priority to the provisional application serial no 60/461,818 filed on April 11, 2003. Applicant invokes swearing back under 37 CFR 1.131, and respectfully submits that the instant invention was made before the Meltzer reference. A Declaration of Prior Invention under 37 CFR 1.131 is submitted along with this response. Further, the invention was made in India, which is a WTO member since January 1, 1995.

One of the evidences to the fact is a Business Plan prepared by the Applicant before the Meltzer's alleged publication date. Further, a non-disclosure agreement (NDA) signed for discussing the Business Plan with an industry expert, Dr. K. Ramdass, was also signed earlier. Both the Business Plan document and the NDA have been presented as exhibits with the Declaration. These are only a few documents that establish that the Applicant was in possession of the instant invention much before the publication of Meltzer. For example, on Page 10, section 5, the Applicant describes an aspect of the idea as thus:

> "... The product will consist of a VA component, another component that fixes security holes automatically, and a third component that tracks services and their configuration files via hooks, and signals to the first two components when a particular configuration changes or a particular service gets started. The first two components then take over, figure out what new vulnerabilities have been created, and fix them automatically. The aspect of tracking services all the time, and dynamically intimating the VA tool and fixing

the vulnerabilities automatically is entirely new and is the real value-add in all this. This idea should be patentable..."

The above lines indicate that the concept of tracking (start and stop of) services, and tracking changes in configurations with the help of hooks (which can be implemented as an agent), and subsequent vulnerability assessment tests to find what new vulnerabilities have been created when new services are started or existing services reconfigured, was in the possession of the Applicant as of January 3, 2003, which is prior to Meltzer's FAQ which was allegedly disclosed on January 30, 2003.

Further, on page 14, section 7, the Applicant describes another aspect of the idea as:

"**7.3 The Services-tracker component**

The key component in the product is the services-tracker component. This component tracks, using hooks, whenever a particular service that accesses a UDP, TCP port or one accessing the IP protocol is started, or if configuration files of such services are changed. It also tracks whether passwords of services that are accessible from the network are changed. This technology is being currently developed via a prototype and should be patentable."

As is understood in the art, one way to implement the hooks is via an agent. Therefore the above supports that the inventor was in possession of the invention before the alleged date of the Meltzer article.

Documents pertaining to the above to support the sequence of events, up to the time of filing of the provisional patent, in addition to those provided with the declaration may made available if required by the respected Examiner.

35 U.S.C. § 103(a)

Meltzer in view of Bunker

Claims 1-38 were rejected under 35 USC 103(a) as being obvious over Meltzer in view of Bunker. This ground of rejection is respectfully traversed because the combination of Meltzer and Bunker do not teach all the elements of the claimed invention, and further, the rejection over Meltzer is overcome by swearing back under the provisions of 37 CFR 1.131.

Applicant has invoked the provision of swearing back because the Applicant believes that the claimed invention was made by the Applicant prior to Meltzer. Further, the Applicant respectfully submits that despite the similarities alleged by the Office Action, the combination of Meltzer and Bunker does not render the instant claims obvious.

For example, with respect to claims 1, 3, 15, 16, 29 and 30, Meltzer does not teach or suggest running *vulnerability assessment tests on the host/device in the event of a change in the status of interface/ports* as claimed in the instant invention. More specifically, Applicant traverses the Office Action allegation that Meltzer (page 5, 1.6 How does a VDS protect my network? Pages 6-12, 2 How do Vulnerability Detection Systems work?) teach running VA tests in the event of a change in the status of interfaces/ports. Applicant respectfully submits that Meltzer does not teach the above mentioned limitation. For example, running VA tests in the event of a change in the status of interfaces/ports comprises running VA tests on services that are started. Meltzer does not teach that vulnerability tests that are run will pertain to the services that are started. Specifically, see Applicants amended specification, paragraph [0020], [0049], [0050], [00176], among others.

For instance, in Meltzer's FAQ, the only sections that deal with this are a) section 2.1 What are continous vulnerability assessments? and b) section 2.6 how do you integrate change detection and vulnerability assessment? In both the cases, Meltzer does not talk about running only specific tests depending on the changes in the status of ports and interfaces. Meltzer merely talks about running a VA tool in a while loop, while importantly, embodiments of the invention provide running only those VA tests as needed.

Bunker does not supply the above noted deficiencies of Meltzer. Accordingly, claims 1, 3, 15, 16, 29 and 30 are believed to allowable under 35 USC over Meltzer in view of Bunker. Claims 2, 4-14, 17-28, and 31-38 that depend directly or indirectly from either of claims 1, 3, 15, 16, 29 or 30, are also believed to be allowable for similar reasons.

In view of the above, Applicant submits that the obviousness rejection over Meltzer in view of Bunker is respectfully traversed. Accordingly, the claims 1-38 are now believed to be allowable under 35 USC 103 (a).

Gleichauf in view of Barnett

Claims 1, 3, 15-16 and 29-30 were rejected under 35 USC 103(a) as being obvious over Gleichauf in view of Barnett. This ground of rejection is respectfully traversed.

According to the Examiner, Gleichauf teaches a system for real-time vulnerability assessment of a host/device, as taught by the instant invention, except that Gliechauf does not teach the nature of the way vulnerabilities are recorded, which deficiency is fulfilled by Barnett. Applicant respectfully disagrees, and submits that neither Gleichauf nor Barnett, alone or in combination, teach all the elements of the recited claims. Applicant respectfully traverses the Office Action statement that Gleichauf, Fig. 2, item 20 teaches an agent running on a host/device.

Applicant submits that item 20 of Fig. 2, Gleichauf is an NVA engine, which is "coupled" to the network backbone, and does not supply an agent running on the host/device as provided by the instant invention. Further, Applicant submits that Gleichauf is concerned with the general issue of multi-phase vulnerability assessment and accordingly serves a very different objective than from the instant invention, and does not teach, suggest or disclose all the elements of the recited claims, either alone or in combination with Barnett. For example, the real-time vulnerability assessment as claimed in the instant invention is absent in both Gleichauf and Barnett. The agent running on the host/device is configured to determine a change in the status of interfaces and/or of ports on the interfaces of the host/device in substantially real-time, which is not disclosed by either of the applied references.

Establishing a *prima facie* case of obviousness requires all the claimed limitations to be taught by the prior art. Further, it is an error to treat the claim as mere catalog of separate parts, in disregard of the part-to-part relationship that give the claim its meaning. As discussed above, at the very least, the combination of Gleichauf and Barnett do not teach an agent running on a host/device as taught by the instant invention. Further, Applicant respectfully submits that Gleichauf is concerned with a different problem, and there exists no teaching, suggestion or motivation in either of the applied references for the combination to arrive at the claimed structure.

Accordingly, independent claims 1, 3, 15-16 and 29-30 are believed to be allowable over Gleichauf in view of Barnett. Claims 2, 4-14, 17-28 and 31-38 that depend directly or indirectly from claims 1, 3, 15-16 and 29-30 are therefore believed to be allowable.

CONCLUSION

In view of the foregoing, Applicant respectfully submits that the application is in condition for allowance. Favorable reconsideration and prompt allowance of the application are respectfully requested.

Should the Examiner believe that anything further is needed to place the application in even better condition for allowance, the Examiner is requested to contact Applicant at the telephone number below.

Respectfully submitted by,

/Dr. Samir G. Kelekar/

Dr. Samir Gurunath Kelekar
Applicant

7/3 Eashwar Jyoti
Krishna Reddy Colony
Domlur Layout Domlur
Bangalore 560071
INDIA

Telephone: +91.80.4125.6233
Mobile: +91 984 504 4403